中華民國經濟部智慧財產局

INTELLECTUAL PROPERTY OFFICE
MINISTRY OF ECONOMIC AFFAIRS
REPUBLIC OF CHINA

茲證明所附文件，係本局存檔中原申請案的副本，正確無訛，
其申請資料如下 ：

This is to certify that annexed is a true copy from the records of this office of the application as originally filed which is identified hereunder :

申　請　日：西元 2003 年 08 月 22 日
Application Date

申 請 案 號：092123183
Application No.

申　請　人：財團法人工業技術研究院
Applicant(s)

局　　長
Director General

蔡 練 生

發文日期：西元 2003 年 9 月 18 日
Issue Date

發文字號：09220939580
Serial No.

申請日期：	IPC分類
申請案號：	

(以上各欄由本局填註)

發明專利說明書

一、發明名稱	中 文	安全政策資料庫之查詢方法
	英 文	
二、發明人(共2人)	姓 名(中文)	1.林俊毅 2.陳官辰
	姓 名(英文)	1. 2.
	國 籍(中英文)	1.中華民國 TW 2.中華民國 TW
	住居所(中 文)	1.雲林縣斗六市梅林里12鄰梅林路147號 2.高雄縣橋頭鄉站前街30號
	住居所(英 文)	1. 2.
三、申請人(共1人)	名稱或姓 名(中文)	1.財團法人工業技術研究院
	名稱或姓 名(英文)	1.
	國 籍(中英文)	1.中華民國 TW
	住居所(營業所)(中 文)	1.新竹縣竹東鎮中興路4段195號 (本地址與前向貴局申請者相同)
	住居所(營業所)(英 文)	1.
	代表人(中文)	1.翁政義
	代表人(英文)	1.

四、中文發明摘要　(發明名稱：安全政策資料庫之查詢方法)

一種安全政策資料庫之查詢方法，主要係根據網際網路安全通訊協定的對等式特性，將原先之安全政策資料庫分割成多個較小之對等式安全政策資料庫，並建立一個對應到對等式安全政策資料庫之對等式目錄。當需要查詢資料庫之政策時，可直接利用本發明對等式安全政策資料庫，節省資料尋找時間。

五、(一)、本案代表圖為：第　六　圖

(二)、本案代表圖之元件代表符號簡單說明：

S30:開始

S32:建立對等式目錄

S34:建立對等式安全政策資料庫

S40:結束

六、英文發明摘要　(發明名稱：)

A method for searching Peer-based security policy database(SPD) exploits the peer-based property of the Internet security policy database. The original SPD is divided into several smaller ones, a Peer-based catalog is established corresponding to the peer-based SPD.The method according to the present invention can advantageously reduce searching time.

一、本案已向

國家(地區)申請專利	申請日期	案號	主張專利法第二十四條第一項優先權

無

二、□主張專利法第二十五條之一第一項優先權:

申請案號:

無

日期:

三、主張本案係符合專利法第二十條第一項□第一款但書或□第二款但書規定之期間

日期:

四、□有關微生物已寄存於國外:

寄存國家:

寄存機構:

無

寄存日期:

寄存號碼:

□有關微生物已寄存於國內(本局所指定之寄存機構):

寄存機構:

寄存日期:

無

寄存號碼:

□熟習該項技術者易於獲得,不須寄存。

五、發明說明 (1)

【發明所屬之技術領域】

一種安全政策資料庫之查詢方法，尤指一種針對網際網路安全通訊協定中之安全政策資料庫，所提出之對等式安全政策資料庫之查詢方法。

【先前技術】

虛擬私人網路(Virtual Private Network; VPN)是利用網際網路協定(Internet Protocol; IP)的技術，建立網際網路上的加密通道(tunneling)來架構網際網路上的企業網路，網際網路協定所建構的網路擴充性良好，所使用的加密技術是標準的網際網路安全通訊協(IP Security)方式，網際網路安全通訊協定結合了加(encryption)、認證(authentication)、密鑰管理(key management)、數位檢定(digital certification)等安全標準，具有高度的保護能力。

當利用網際網路安全通訊協定執行資料傳送時，根據傳輸資料的方向可分為向內處理(inbound processing)跟向外處理(outbound processing)。向內處理是指由對等網路(peer net)，經過對等閘道(peer gateway)，送至本地閘道(local gateway)，最後到本地網路(local net)；向內處理收到的封包(packet)稱為向內封包(inbound packet)，向內封包有兩種，一種是經過網際網路安全通訊協定處理過的向內網際網路安全通訊協定封包(inbound IPSec packet)，另一種是普通的向內網際網路協定封包(inbound IP packet)。向外處理是指由本地網路，經過

本地閘道，送至對等閘道，最後到對等網路；向外處理收到的封包(packet)稱為向外封包(outbound packet)，為一種向外網際網路協定封包(outbound IP packet)。

網際網路安全通訊協定有傳輸模式(transport mode)與通道模式(tunnel mode)兩種不同的模式，傳輸模式為主機對主機(host-to-host)的封裝機制，參與通訊兩端的主機一定要實作網際網路安全通訊協定之傳輸模式；通道模式則是閘道對閘道(gateway-to-gateway)或閘道對主機(gateway-to-host)的封裝機制，只要閘道或主機有實作網際網路安全通訊協定之通道模式即可。換句話說，一台支援網際網路安全通訊協定的主機必須實作傳輸模式與通道模式，閘道只須實作通道模式，不過閘道也可以支援傳輸模式以提供多一種選擇讓閘道本身直接與主機通訊。

網際網路安全通訊協定是依照使用者在安全政策資料庫中，指定的網路位址、傳輸協定和埠號(Port Number)等篩選條件，決定哪些封包是需要特別處理的，處理的方式包括實施(apply)網際網路安全通訊協定、跳過(by-pass)網際網路安全通訊協定和直接丟棄(discard)，內定處理方式為直接丟棄封包。且若要實施網際網路安全通訊協定，使用者還要在安全協議資料庫(Security Association Database; SAD)中，指定網際網路安全通訊協定的模式、網際網路安全通訊協定傳輸協定、驗證演算法、加解密演算法和金鑰等資訊。

其中安全政策是用來制定網際網路安全通訊協定的動

作方式，包含了通訊對象及資料類型、是否加密及加密方式、驗證的方式、是否建立加密通道及對象、區域網路或遠端存取。因此不同的通訊對象、資料類型、驗證及加密的方式即會對應到不同的安全政策。這些不同的政策就組成了一個安全政策資料庫（Security Policy Database; SPD)進行集中管理。

因此，安全政策資料庫為由不同安全政策所組成的一個有順序的串列(ordered list)。每個政策可以根據不同的篩選條件(selector)來挑選，篩選條件包括了來源位址(source address)、目標位址（destination address)、傳輸協定(protocol)、來源埠（source port)以及目標埠(destination port)，而且每個篩選條件範圍值可能是單個(single)、範圍(range)或萬用字元(wildcard)。

由於篩選條件可能相同，所以政策之間就容易產生重疊的情形，即在安全政策資料庫中，可能有兩條以上的政策的篩選條件同時符合一個封包在安全政策資料庫查詢要求。因此，網際網路安全通訊協定有規定安全政策資料庫的查詢必須是有順序性的從頭開始搜尋，直到找到第一個條件符合的政策為止，以獲得一致性的查詢結果。

第一圖為原先安全政策資料庫示意圖(習用技術)。如果直接以線性查詢（linear search)作為查詢安全政策資料庫的方法，其時間複雜度(time complexity)為O(n)，n為政策數目。對於政策數量較大的系統，線性查詢安全政策資料庫將會成為網際網路安全通訊協定處理的瓶頸。目

前商業產品規格中所載的政策數量上限，在家用或小型企業用的設備方面通常在100以下， 中大型企業用設備約為1000，超大型企業用設備則約為10000。

昔用技術中用來解決安全政策資料庫之查詢，有下列三種方法：一種為暴力平行(brute force parallel)安全政策資料庫查詢法；一種為封包流式(Flow-based)安全政策資料庫查詢法(美國專利號6,347,376、美國專利公告號2003/0023846和2003/0069973)，請參照第二圖；另一種為派翠西式(PATRICIA-based)安全政策資料庫查詢法(美國專利號6347376和美國專利公告號2003/0061507)， 請參照第三圖。

暴力平行安全政策資料庫查詢法是直接利用硬體可平行處理的特性，依據系統規格的政策數量除以單一安全政策資料庫模組能處理的最大政策數量值，以決定需要複製多少個安全政策資料庫模組。在此向內封包或向外封包的安全政策資料庫查詢要求，由政策管理者(policy manager)集中管理，再廣播給底下所有的向內封包之安全政策資料庫，或向外封包之安全政策資料庫，同時作查詢作，並回報查詢結果給政策管理者。如果有兩個以上安全政策資料庫都找到符合條件的政策，政策管理者只會選擇最高優先權的政策往上回報。

此方法的缺點是成本較高因為需要複製多個安全政策資料庫模組，且最多只能同時服務兩個安全政策資料庫查詢要求，即一個向內封包安全政策資料庫查詢和一個向外

封包安全政策資料庫查詢。

封包流式安全政策資料庫查詢法會針對每一個封包流作一些特別處裡。以傳輸控制協定 (Transport Control Protocol; TCP) 封包為例，擁有相同來源位址、目標位址、傳輸協定、來源埠以及目標埠的封包被視為屬於同一個封包流。當然每個封包流的第一個封包還是得線性查詢安全政策資料庫，以得到相對應的政策，不過此方法會將查詢結果儲存起來供同一個封包流的其餘封包使用。如果將查詢結果存放在一個空間使用率不超過一半的雜湊表 (hash table)，理論上時間複雜度為 O(1)。

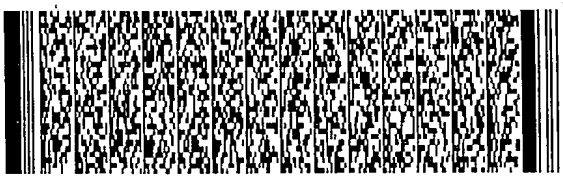
然而此方法的缺點是需要大量的記憶體空間來維持這個散列表，其空間複雜度 (space complexity)為 O(f)，f 為封包流的數量。另外，此方法的第一個封包依然需要線性查詢安全政策資料庫，因此可能會造成應用層網路程式在建立連線前可能會出現有一段延遲時間。

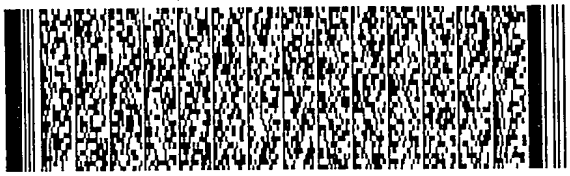
派翠西式安全政策資料庫查詢法使用派翠西樹 (PATRI-CIA Tree)來查詢資料，派翠西樹是一種二元搜尋樹演算法 (binary searching tree algorithm)。有不相鄰面罩 (non-contiguous masks)的派翠西樹的最糟情況 (worst case)為 O(w2)，w為派翠西樹鑰匙 (key)的長度。以美國專利公告號 2003/0061507的方法為例，w為 112。使用派翠西式安全政策資料庫查詢法缺點在於，必須限制所有安全政策資料庫內的政策不能互相重疊或者是需要另一套有效率的演算法先將原先的安全政策資料庫轉換成無順序性 (non

-ordered)的安全政策資料庫，以致於查詢結果才能符合網際網路安全通訊協定所要求的順序性。但是目前所提出的類似方法裡頭皆沒有一併提出轉換安全政策資料庫成無順序性的安全政策資料庫之方法。

第四圖為向外網際網路安全通訊協定處理流程圖（習用技術）。對於向外網際網路協定封包（S10），會先進行安全政策資料庫的查詢（ S12）；如果查詢結果是直接丟棄，則直接把封包丟棄（ S11）；如果查詢結果是跳過網際網路安全通訊協定， 則進入網際網路協定的處理（S13）；如果查詢結果是實施網際網路安全通訊協定，則再查詢安全協議資料庫（ S15）；如果沒有查到，則丟棄封包，並建立安全協議（S14）；如果有查到，則封裝（encapsulation)外部檔頭（S16）；再進行加密（encryption)和認證（ authentication)動作（S17）；然後送入網際網路協定的處（S13）。

第五圖為向內網際網路安全通訊協定處理流程圖 （習用技術）。對於向內網際網路安全通訊協定封包（S20），則要先查詢安全協議資料庫（S23），如果沒有查到（S22），則丟棄封包；如果有查到，先進行解密（decryption)和認證動作（S24）；再解封裝（ decapsulation)外部檔頭（S25）；之後，進行安全政策資料庫的查詢（ S26）。對於向內網際網路協定封包（ S21），則直接進行安全政策資料庫的查詢（S26）。安全政策資料庫的查詢，如果查到是錯誤的策，則直接丟棄封包（S22）；如果查到正確的政策，則進行網際網路協定的處理（S27）。





五、發明說明（7）

【發明內容】

本發明的目的是提供一種安全政策資料庫之查詢法。依據本發明之一特點，本發明根據網際網路安全通訊協定的對等式特性，將原來的安全政策資料庫分割成多個較小的對等式安全政策資料庫，並建立一個對應到對等式安全政策資料庫的對等式目錄，以節省尋找政策的時間。

依據本發明之另一特點，本發明要查詢政策時，會利用政策的篩選條件如：來源位址、或目標位址來查詢對等式目錄中。而在對等式目錄中，符合這個篩選條件會對應一個對等識別碼，這個對等識別碼會對應至一對等式安全政策資料庫。

依據本發明之另一特點，本發明可應用在向內封包，無論是經過網際網路安全通訊協定處理過的向內網際網路安全通訊協定封包，或是普通的向內網際網路協定封包；本發明亦可應用在向外封包，亦即向外網際網路協定封包。

依據本發明之另一特點，本發明可應用在網際網路安全通訊協定之通道模式；亦可支援網際網路安全通訊協定之傳輸模式。

依據本發明之另一特點，本發明可結合暴力平行安全政策資料庫查詢法和封包流式安全政策資料庫查詢法來使用，增進這兩種方法之查詢效果。

【實施方式】

我們以閘道的角度，並以通道模式來說明本發明之具體實例。

一條網際網路安全通訊協定通道可視為由一個起始閘道 (originating gateway)和一個終止閘道 (terminating gateway)所構成的通道。從內部網路 (internal network /Local Area Network; LAN) 往外傳送的向外封包在經過起始閘道的網際網路安全通訊協定處理後，會被加上一層外部檔頭 (outer header)，這層外部檔頭來源位址是起始閘道的位址，目標位址則是終止閘道的位址，此時終止閘道是起始閘道的對等閘道。

若從另一個角度來看同一個封包，終止閘道則將它視為要進入其內部網路的向內封包。在終止閘道解除網際網路安全通訊協定的保護機制後，還原後的封包才會被轉送到真正的目的端主機，此時終止閘道則將起始閘道視為對等閘道。

綜上所述，我們可以推論得知：在向內網際網路安全通訊協定封包的之外部檔頭中，來源位址就是對等閘道的外部網路 (external network/Wide Area Network; WAN) 的位址；在向內網際網路協定封包的檔頭 (header)中，來源位址則是位於對等閘道的內部網路之內；而在向外網際網路協定的內部檔頭中，目標位址則是位於對等閘道的內部網路之內

因此，我們可以善用這種對等閘道與封包之間的係，建立一個對等式目錄 (peer table)，並為每個對等閘道建

立一對等式安全政策資料庫(peer SPD)以加快安全政策資料庫的查詢速度。

第六圖A為本發明安全政策資料庫查詢方法流程圖。方法開始(S30);首先要建立一個對等式目錄(S32);然後根據對等式等目錄中的每個對等閘道,建立其專屬對等式安全政策資料庫(S34);第六圖B則是等到要查詢安全政策的時候的流程,就先查詢對等式目錄(S36),找到對應之對等式安全政策資料庫;然後再查詢對等式安全政策資料庫(S38);進而找到安全政策;最後整個方法結束(S40)。第七圖為本發明對等式目錄示意圖。這個對等式目錄至少包含以下的欄位:對等識別碼(peer identification)、位址(address)、前置屬性(prefix)和型別(type)。

對等識別碼是指向其對應之對等式安全政策資料庫的指標(pointer)。位址是內部網路區段或是外部網路址。前置屬性則代表:要比對位址中多少位元(bit),才算找到相符的位址。型別有三種,分別是I(內部網路區段型別)、E(外部網路位址型別)以及B(兩者皆是)。以網際網路協定版本4(IP version 4; IPv4)為例,外部網路位址對應之前置屬性的長度為32;內部網路位址對應之前置屬性的長度的範圍則介於1到32之間,視實際網路大小而定。而外部位址的前置屬性長度應與位址位元數目相同。

每個對等閘道在對等式目錄至少建立兩筆的資料,分別以位址、前置屬性與型別來表示對等閘道的外部網路位址以及其內部網路區段。第七圖中,對等識別碼1的對等

閘道，外部網路位址即為203.56.77.33，內部網路區段為140.96.0.0且前置屬性為16，代表由140.96.0.0到140.96.255.255。同樣地對等識別碼2的對等閘道，外部網路位址即為207.52.79.40，內部網路區段為140.112.0.0且前置屬性為16，代表從140.112.0.0到140.112.255.255。此外，對等識別碼0的對等閘道為一個預設的對等閘道(default peer gateway)，供其餘無法對應得到對等閘道之封包使用，其位址與前置屬性皆為0，型別為B。

第八圖為本發明對等式安全政策資料庫示意圖。本發明為每個對等閘道建立一個專屬的安全政策資料庫，稱為對等式安全政策資料庫，只儲存與這個對等閘道相關的安全政策。預設的對等閘道也有一個專屬的對等式安全政策資料庫，但只用來存放跳過的政策與直接丟棄的政策。第一圖中，原先的安全政策資料庫(original SPD)是採取線性排列的方式。而在為每個對等閘道建立一個專屬的安全政策資料庫後，就如第八圖所示，與對等識別碼1的對等閘道相關的安全政策只有1跟5；與對等識別碼2的對等閘道相關的安全政策為2、3、跟4；與對等識別碼0的對等閘道相關的安全政策為3。這些適用於不同對等閘道的安全政策，分別以一個線性排列方式，形成獨立的對等式安全政策資料庫資料庫。

當要搜尋第一圖的安全政策時，需要從1搜尋到5。如果搜尋第八圖的安全政策，只要先從對等式目錄找到對等識別碼，然後搜尋其對應的對等式安全政策資料庫，所要

搜尋的安全政策數量將減少許多，而節省搜尋安全政策的時間。

當使用者新增政策時，除了加入原先的安全政策資料庫外，若是通道模式下的安全政策，則依照政策的對等閘道位址去查詢對等式目錄以找到對等識別碼，然後加入相對應的對等式安全政策資料庫。而且為了保持與原先的安全政策資料庫一致的政策順序性，所有被新增的政策還要視其篩選條件是否與其他對等閘道的內部網路區段重疊，每一個與此政策（通常是跳過的政策與直接丟棄的政策）發生重疊的對等閘道必須將之加入其對等式安全政策資料庫之內。

當使用者要刪除政策，必須同時移除該政策在原先的安全政策資料庫，以及對等式安全政策資料庫內的資料。如果要同時支援傳輸模式，原則上我們只須將每一個與閘道直接通訊的對等主機(Peer Host)皆視為對等閘道可。

首先為每個對等主機在對等式目錄建立至少一筆料，存放對等主機的網路位址，其前置屬性與位址位元數相同，且型別為B。每個對等主機也有一個專屬的對等式安全政策資料庫，同樣地都是使用上述的方法建置而成，儘管傳輸模式下，政策本身並沒有對等閘道位址的資訊，但是因為傳輸模式下，政策的篩選條件之目標位址或來源位址會因為和對等主機發生重疊關係，而落入其對等式安全政策資料庫內。

在傳輸模式下，向內網際網路協定封包和向外網際網

路協定封包的安全政策資料庫查詢方式，與通道模式是相同的；而向內網際網路協定安全封包，在傳輸模式下的安全政策資料庫查詢方式，則與通道模式不同。

以下分別介紹：通道模式的向內網際網路安全通訊協定封包處理流程；傳輸模式的向內網際網路安全通訊協定封包處理流程；向內網際網路協定封包處理流程；及向外網際網路協定封包處理流程。

第九圖為本發明處理通道模式下的向內網際網路安全通訊協定封包(inbound IPSec packet)之流程圖。對於向內網際網路安全通訊協定封包，首要步驟為解除網際網路安全通訊協定的保護(S100)；然後用向內網際網路安全通訊協定封包的外部檔頭之來源位址，去比對對等式目錄的外部網路位址(S102)，以得到相對應的對等式安全政策資料庫；如果找不到，則代表找不到政策(S108)；反之，代表得到相對應的對等式安全政策資料庫，則比對向內網際網路安全通訊協定封包的內部檔頭與對等式安全政策資料庫內的政策(S104)，以得到條件符合的政策；如果條件符合，則找到政策(S106)；否則，代表找不到政策(S108)。第十圖為本發明處理傳輸模式下的向內網際網路安全通訊協定封包(inbound IPSec packet)之流程圖。對於向內網際網路安全通訊協定封包，首要步驟為解除網際網路安全通訊協定的保護(S200)；然後用向內網際網路安全通訊協定封包之來源位址，去比對對等式目錄的外部網路位址(S202)，以得到相對應的對等式安全政策資料庫；如果找

不到，則代表找不到政策（S208）；反之，代表得到相對應的對等式安全政策資料庫，則比對向內網際網路安全通訊協定封包與對等式安全政策資料庫內的政策（S204），以得到條件符合的政策；如果條件符合，則找到政策（S206）；否則，代表找不到政策（S208）。

第十一圖為本發明處理向內網際網路協定封包（inbound IP packet)之流程圖。先用向內網際網路協定封包之來源位址，去比對對等式目錄的內部網路區段（S300），以得到相對應的對等式安全政策資料庫；如果找不到，則代表找不到政策（S306）；反之，代表得到相對應的對等式安全政策資料庫，則比對向內網際網路協定封包與對等式安全政策資料庫內的政策（S302），以得到條件符合的政策；如果條件符合，則找到政策（S304）；否則，代表找不到政策（S306）。

第十二圖為本發明處理向外網際網路協定封包（outbound IP packet)之流程圖。先用向外網際網路協定封包之目標位址，去比對對等式目錄的內部網路區段（S400），以得到相對應的對等式安全政策資料庫；如果找不到，則代表找不到政策（S406）；反之，代表得到相對應的對等式安全政策資料庫，則比對向外網際網路協定封包與對等式安全政策資料庫內的政策（S402），以得到條件符合的政策；如果條件符合，則找到政策（S404）；否則，代表找不到政策（S406）。

另外，本案發明還可以結合其他改良過的安全政策資

料庫查詢方法，如：暴力平行安全政策資料庫查詢法和封包流式安全政策資料庫查詢法。直接將這兩種方法應用在所有的對等式安全政策資料庫，甚至選擇性的應用在某些對等式安全政策資料庫上，如資料流量較大的對等閘道。

當結合暴力平行安全政策資料庫查詢法時，可將向內封包之安全政策資料庫和向外封包之安全政策資料庫，都利用本發明所提出的方法，分成數個較小的向內封包之對等式安全政策資料庫，以及數個較小的向外封包之對等式安全政策資料庫。再由政策管理者(policy manager)集中管理，針對每個查詢要求只轉送給相關的數個向內封包之對等式安全政策資料庫，或數個向外封包之對等式安全政策資料庫，同時作查詢動作，便可同時服務多個不同對等閘道的安全政策資料庫查詢要求，進一步的提升系統效能。

當結合封包流式安全政策資料庫查詢法時，可將每個封包流的第一個封包，要線性查詢安全政策資料庫的步驟，改成查詢對等式安全政策資料庫，減少因查詢所造成時間的延遲。

本發明雖然多了一項尋找對等閘道的工作，但是無論是使用軟體或硬體方法，尋找對等閘道的時間複雜度都只為O(1)。如此一來卻可以換來一個平均政策數量只為原來安全政策資料庫的1/p的對等式安全政策資料庫，p為對等閘道的數目，因此查詢安全政策資料庫的時間複雜度在一般狀況(average case)時降為O(n/p)。

五、發明說明（15）

本發明已以較佳實施例說明如上，熟習該項技術者皆得對該等實施例加以變化，且如此構成之變化實施例在精神與範圍上皆不脫離本發明之範圍，本發明之範圍定義於下述申請專利範圍中。

圖式簡單說明

第一圖為原先安全政策資料庫示意圖（習用技術）；

第二圖為封包流式安全政策資料庫查詢法（習用技術）；

第三圖為派翠西式安全政策資料庫查詢法（習用技術）；

第四圖為向外網際網路安全通訊協定處理流程圖（習用技術）；

第五圖為向內網際網路安全通訊協定處理流程圖（習用技術）；

第六圖A及第六圖B為本發明安全政策資料庫查詢方法流程圖；

第七圖為本發明對等式目錄示意圖；

第八圖為本發明對等式安全政策資料庫示意圖；

第九圖為 本發明處理通道模式下的向內網際網路安全通訊協定封包（inbound IPSec packet)之流程圖；

第十圖為本發明處理傳輸模式下的向內網際網路安全通訊協定封包（inbound IPSec packet)之流程圖；

第十一圖為本發明處理向內網際網路協定封包（inbound IP packet)之流程圖；

第十二圖為本發明處理向外網際網路協定封包（outbound IP packet)之流程圖。

【元件代表符號簡單說明】

S10向外網際網路封包

S11丟棄封包

S12安全政策資料庫查詢

圖式簡單說明

S13網際網路封包處理

S14丟棄封包和建立安全協議

S15安全協議資料庫查詢

S16封裝外部檔頭

S17加密和驗證

S20向內網際網路安全通訊封包

S21向內網際網路封包

S22丟棄封包

S23安全協議資料庫查詢

S24解密和驗證

S25解封裝外部檔頭

S26安全政策資料庫查詢

S27網際網路封包處理

S30開始

S32建立對等式目錄

S34建立對等式安全政策資料庫

S36查詢對等式目錄

S38查詢對等式安全政策資料庫

S40結束

S100解除安全保護

S102比對封包外部檔頭之來源位址與對等式目錄之外部網路位址

S104比對封包內部檔頭與對等式安全政策資料庫

S106找到政策

圖式簡單說明

S108找不到政策

S200解除安全保護

S202比對封包來源位址與對等式目錄之外部網路位址

S204比對封包與對等式安全政策資料庫

S206找到政策

S208找不到政策

S300比對封包來源位址與對等式目錄之內部網路區段

S302比對封包與對等式安全政策資料庫

S304找到政策

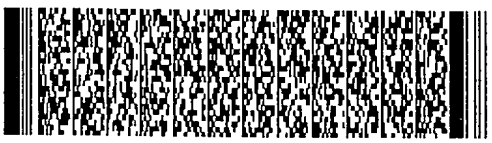
S306找不到政策

S400比對封包目標位址與對等式目錄之內部網路區段

S402比對封包與對等式安全政策資料庫

S404找到政策

S406找不到政策



六、申請專利範圍

1.一種安全政策資料庫之查詢方法，至少包含下列步驟：

建立一對等式目錄；

建立一組對等式安全政策資料庫，係由複數個對等式安全政策資料庫所組成；

查詢該對等式目錄，可得一對應之對等式安全政策資料庫；及

查詢該對應之對等式安全政策資料庫，獲取一安全政策。

2.如申請專利範圍第 1項所述之安全政策資料庫之查詢方法，其中該建立一對等式目錄之步驟中，更包含根據一對等閘道（Peer Gateway），於該對等式目錄中建立至少二筆資料；若根據一組對等閘道，則可於該對等式目錄中建立至少二組資料。

3.如申請專利範圍第 2項所述之安全政策資料庫之查詢方法，其中該至少二筆資料中，一為內部網路資料，另一為外部網路資料；另該至少二組資料係為一組內部網路資料和一組外部網路資料。

4.如申請專利範圍第 3項所述之安全政策資料庫之查詢方法，其中該內部網路資料或外部網路資料係至少包含一對等式識別碼、一位址、型別、及一前置屬性；該對等式識別碼係代表該對等閘道；該位址一內部網路位址，該型別為內部網路區段型別、外部網路位址型別或兩者皆是；該前置屬性為比對位址位元數。

5.如申請專利範圍第 4項所述之安全政策資料庫之查詢方

六、申請專利範圍

法，其中該內部網路資料包含之位址為內部網路區段。

6.如申請專利範圍第 4項所述之安全政策資料庫之查詢方法，其中該外部網路資料包含之位址為一外部網路位址。

7.如申請專利範圍第 1項所述之安全政策資料庫之查詢方法，其中該建立一對等式目錄之步驟，係更包含根據一預設對等閘道之步驟，係於該對等式目錄另建立一筆資料，而該資料係至少包含一對等式識別碼、一位址、型別、及一前置屬性；其中該對等式識別碼為0、該位址為0、及該前置屬性為0者。

8.如申請專利範圍第 1項所述之安全政策資料庫之查詢方法，其中該建立一組對等式安全政策資料庫之步驟，係更包含有一根據一對等閘道而建立一對等式安全政策資料庫之步驟，係儲存與該對等閘道相關之安全政策；此步驟係另可根據複數個對等閘道，進而建立複數個對等式安全政策資料庫。

9.如申請專利範圍第 1項所述之安全政策資料庫之查詢方法，其中該建立一組對等式安全政策資料庫之步驟，係更包含根據一預設之對等閘道而建立一預設對等式安全政策資料庫之步驟，係儲存與該預設對等閘道相關之安全政策。

10.如申請專利範圍第 8項所述之安全政策資料庫之查詢方法，其中該根據一對等閘道建立之該對等式安全政策資料庫步驟，係根據一安全政策之一篩選條件，而該

六、申請專利範圍

篩選條件係為一來源位址或為一目標位址者。

11.如申請專利範圍第9項所述之安全政策資料庫之查詢方法，其中與該預設對等閘道有關的安全政策，係為一跳過的安全政策，或為一直接丟棄之安全政策者。

12.如申請專利範圍第1項所述之安全政策資料庫之查詢方法，其中該建立一組對等式安全政策資料庫之步驟，係更包含一加入安全政策之方法，該方法至少包括：

將該安全政策依照一篩選條件，而加入該組對等式安全政策資料庫之中。

13.如申請專利範圍第12項所述之安全政策資料庫之查詢方法，其中該篩選條件為一來源位址或為一目標位址者。

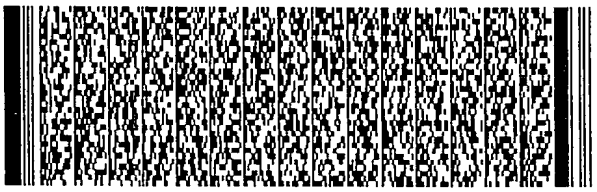
14.如申請專利範圍第1項所述之安全政策資料庫之查詢方法，其中該建立一組對等式安全政策資料庫之步驟，係更包含一刪除安全政策之方法，至少包括：

將該安全政策依照一篩選條件，自該組對等式安全政策資料庫中刪除。

15.如申請專利範圍第14項所述之安全政策資料庫之查詢方法，其中該篩選條件係為一來源位址或為一目標位址者。

16.如申請專利範圍第1項所述之安全政策資料庫之查詢方法，其中該查詢對等式目錄之步驟中，係包含一比對一封包與該對等式目錄之步驟者。

17.如申請專利範圍第16項所述之安全政策資料庫之查詢



六、申請專利範圍

方法，其中該封包係可為一通道模式下之一向內網際網路安全通訊協定封包者；則該比對步驟，係比對該通道模式下之向內網際網路安全通訊協定封包之外部檔頭之來源位址與該對等式目錄之外部網路位址。

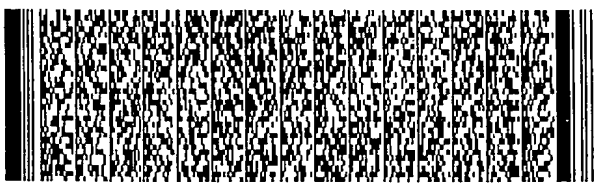
18.如申請專利範圍第16項所述之安全政策資料庫之查詢方法，其中該封包係為一傳輸模式下之向內網際網路安全通訊協定封包者；則該比對步驟，係比對該傳輸模式下之向內網際網路安全通訊協定封包之來源位址與該對等式目錄之外部網路位址。

19.如申請專利範圍第16項所述之安全政策資料庫之查詢方法，其中該封包係為一向內網際網路協定封包者；則該比對步驟係比對該向內網際網路協定封包之來源位址與該對等式目錄之內部網路區段。

20.如申請專利範圍第16項所述之安全政策資料庫之查詢方法，其中該封包係為一向外網際網路協定封包者；則該比對步驟係比對該向外網際網路協定封包之目標位址與該對等式目錄之內部網路區段。

21.如申請專利範圍第1項所述之安全政策資料庫之查詢方法，其中該查詢該對等式安全政策資料庫之步驟，係包含比對一封包與該對等式安全政策資料庫之步驟者。

22.如申請專利範圍第21項所述之安全政策資料庫之查詢方法，其中該封包可為一通道模式下之向內網際網路安全通訊協定封包；則該比對步驟係比對該通道模式



六、申請專利範圍

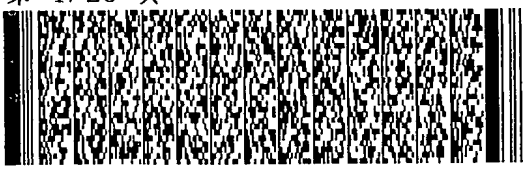
下之向內網際網路安全通訊協定封包解除安全封裝後之內部檔頭與該對等式安全政策資料庫之安全政策之篩選條件。

23.如申請專利範圍第21項所述之安全政策資料庫之查詢方法，其中該封包係可為一傳輸模式下之向內網際網路安全通訊協定封包；則該比對步驟係比對該通道模式下之向內網際網路安全通訊協定封包解除安全封裝後之檔頭與該對等式安全政策資料庫之安全政策之篩選條件。

24.如申請專利範圍第21項所述之安全政策資料庫之查詢方法，其中該封包係可為一向內網際網路協定封包；則該比對步驟係比對該向內網際網路協定封包之檔頭與該對等式安全政策資料庫之安全政策之篩選條件。

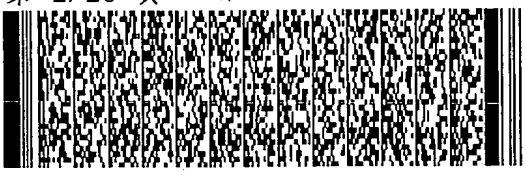
25.如申請專利範圍第21項所述之安全政策資料庫之查詢方法，其中該封包係可為一向外網際網路協定封包；則該比對步驟係比對該向外網際網路協定封包之檔頭與該對等式安全政策資料庫之安全政策之篩選條件。

第 1/26 頁



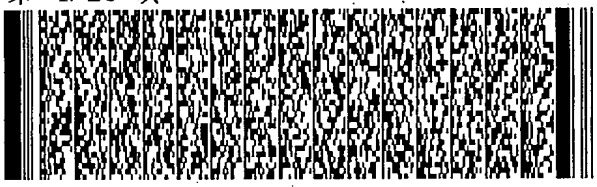
第 2/26 頁

第 2/26 頁



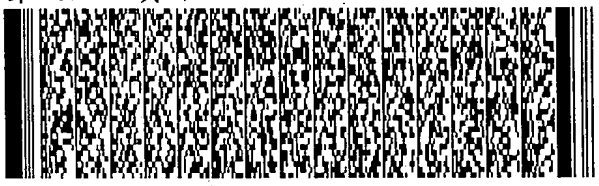
第 3/26 頁

第 4/26 頁



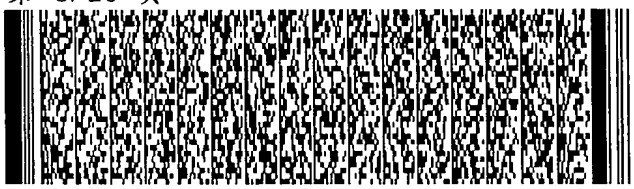
第 4/26 頁

第 5/26 頁

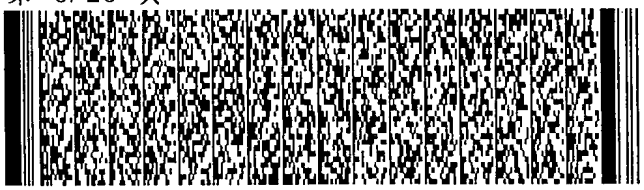


第 5/26 頁

第 6/26 頁

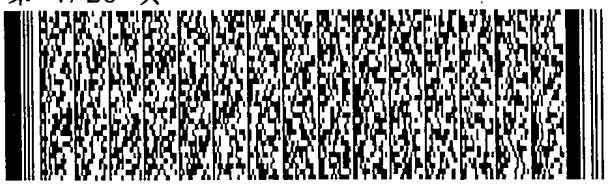


第 6/26 頁

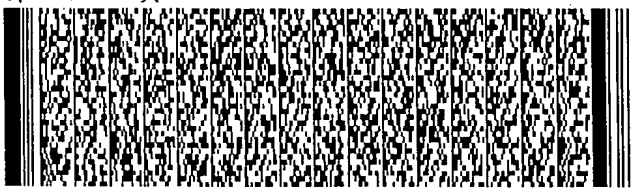


第 7/26 頁

第 7/26 頁



第 8/26 頁

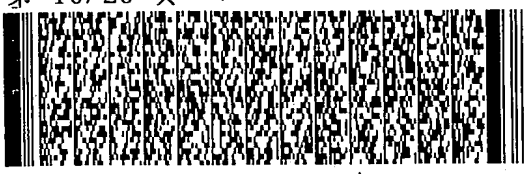


第 8/26 頁

第 9/26 頁

第 9/26 頁

第 10/26 頁

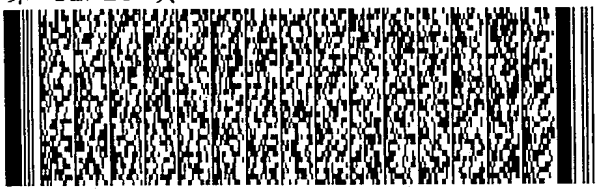


第 10/26 頁

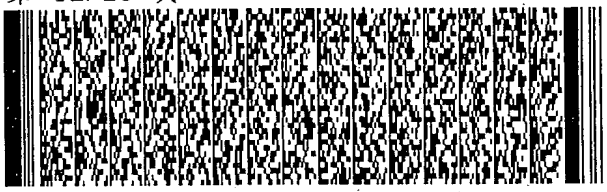
第 11/26 頁

第 11/26 頁

第 12/26 頁



第 12/26 頁

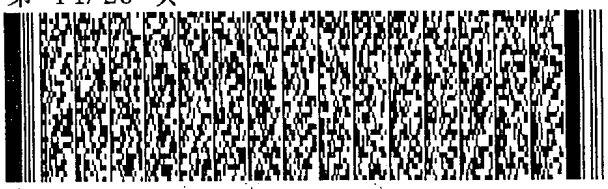


第 13/26 頁

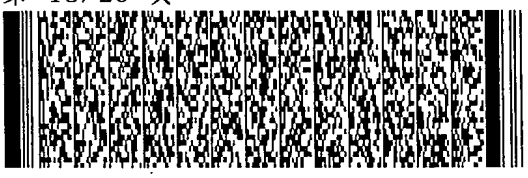
第 13/26 頁

第 14/26 頁

第 14/26 頁



第 15/26 頁



第 15/26 頁

第 16/26 頁

第 17/26 頁

第 17/26 頁

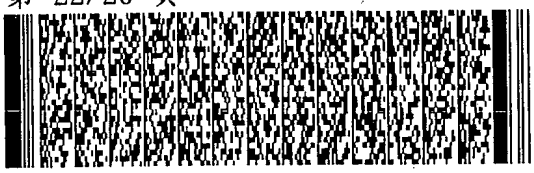
第 18/26 頁

第 19/26 頁

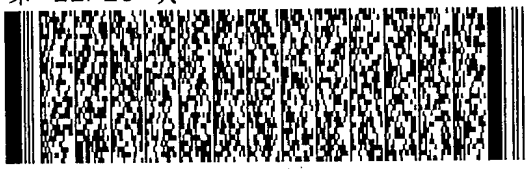
第 20/26 頁

第 21/26 頁

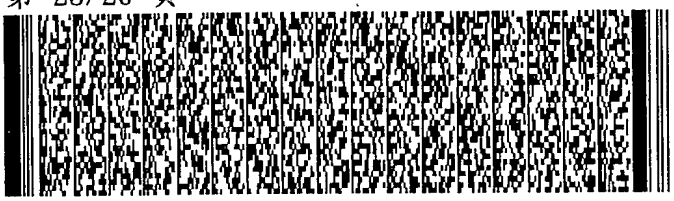
第 22/26 頁



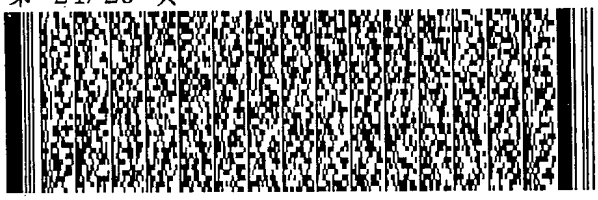
第 22/26 頁



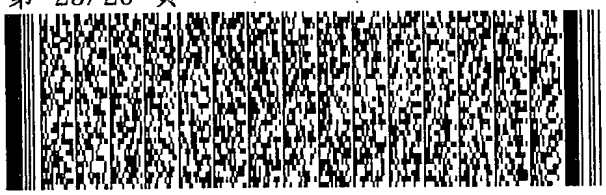
第 23/26 頁



第 24/26 頁



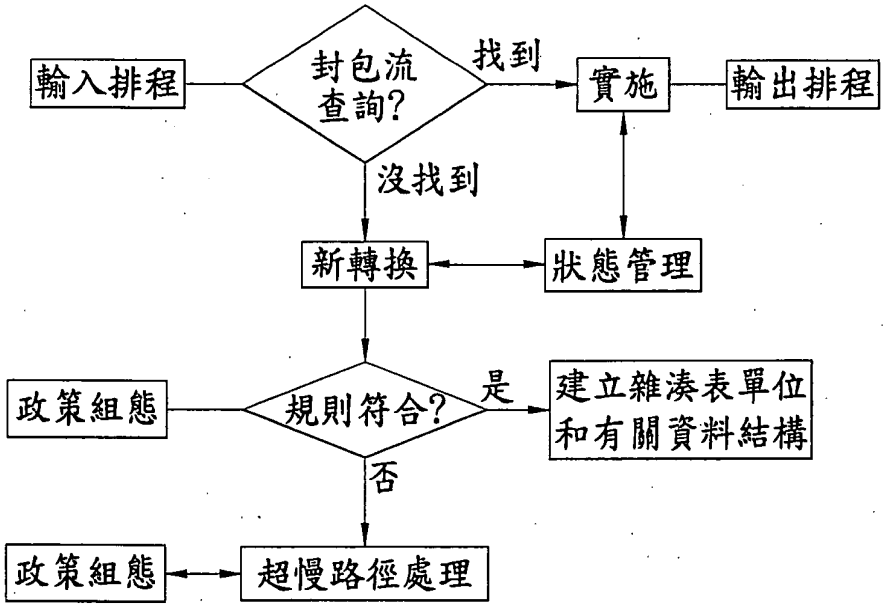
第 25/26 頁



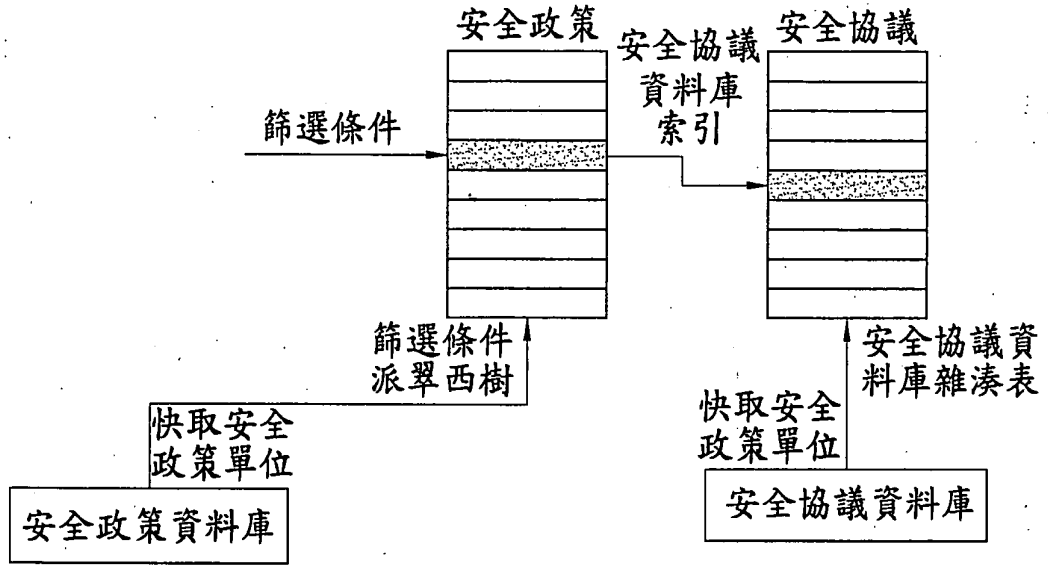
第 26/26 頁

原本的安全政策資料庫

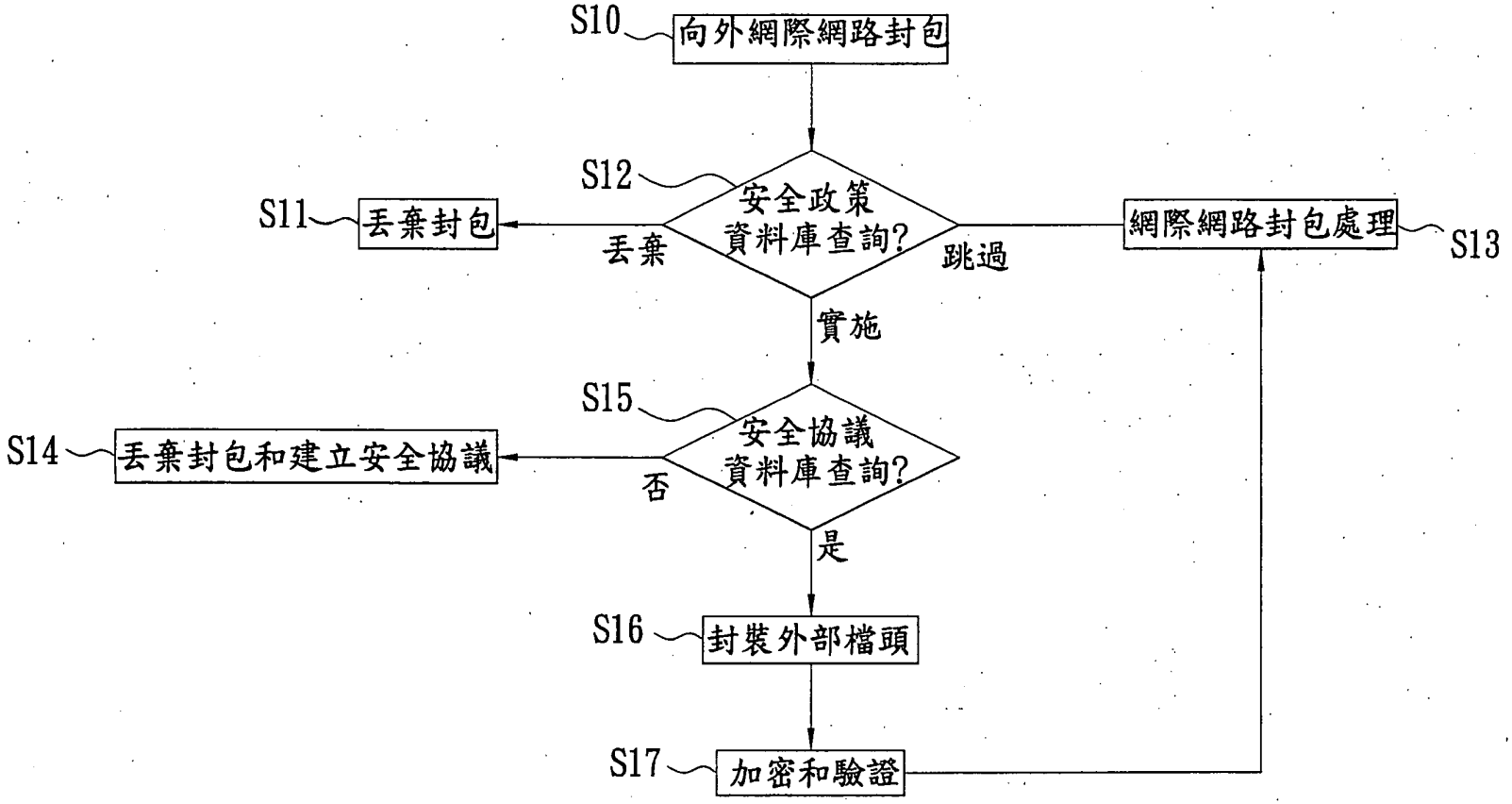
第一圖
（習用技術）


輸入排程
封包流查詢?
找到
實施
輸出排程
沒找到
新轉換
狀態管理
政策組態
規則符合?
是
建立雜湊表單位和有關資料結構
否
政策組態
超慢路徑處理

第二圖
（習用技術）

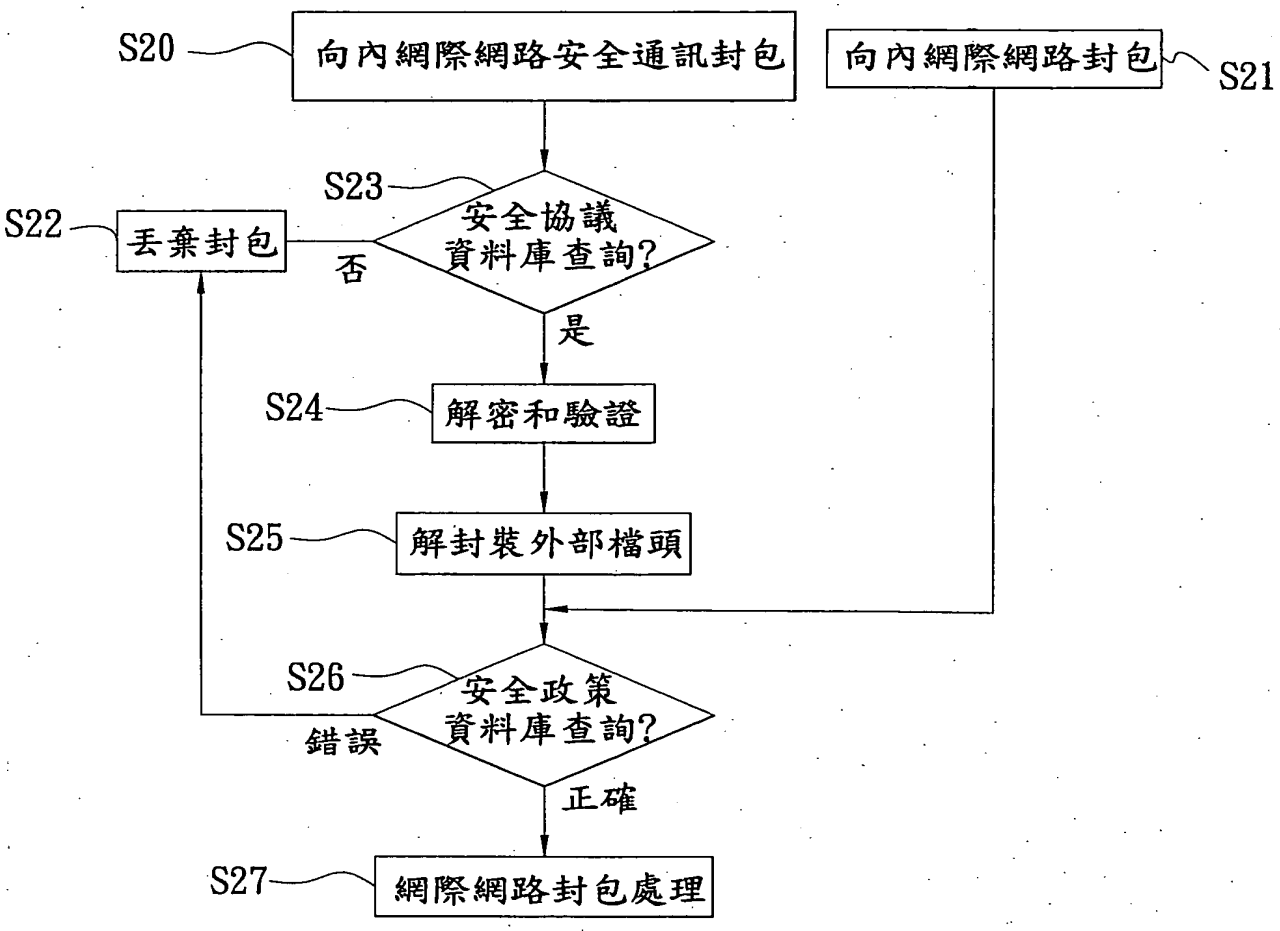

安全政策
安全協議資料庫索引
安全協議
篩選條件
篩選條件派翠西樹
安全協議資料庫雜湊表
快取安全政策單位
快取安全政策單位
安全政策資料庫
安全協議資料庫

第三圖
（習用技術）


S10
向外網際網路封包
S12
安全政策
資料庫查詢?
S11
丟棄封包
丟棄
跳過
網際網路封包處理
S13
實施
S15
安全協議
資料庫查詢?
S14
丟棄封包和建立安全協議
否
是
S16
封裝外部檔頭
S17
加密和驗證

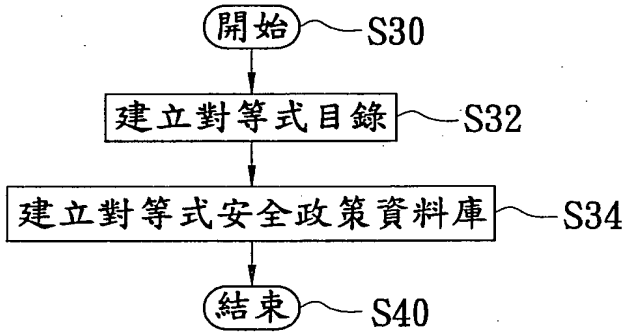
第四圖
（習用技術）

圖式


S20
向內網際網路安全通訊封包
向內網際網路封包
S21
S23
安全協議
資料庫查詢?
S22
丟棄封包
否
是
S24
解密和驗證
S25
解封裝外部檔頭
S26
安全政策
資料庫查詢?
錯誤
正確
S27
網際網路封包處理

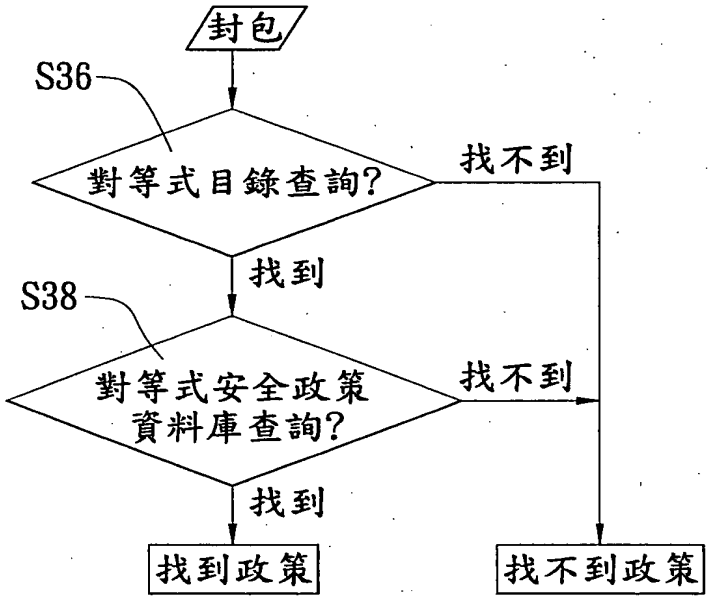
第五圖
（習用技術）

圖式



第六圖A

圖式



第六圖B

對等識別碼	位址	前置屬性	型別
1	203.56.77.33	32	E
1	140.96.0.0	16	I
2	207.52.79.40	32	E
2	140.112.0.0	16	I
0	0.0.0.0	0	B

第七圖

對等式安全政策資料庫

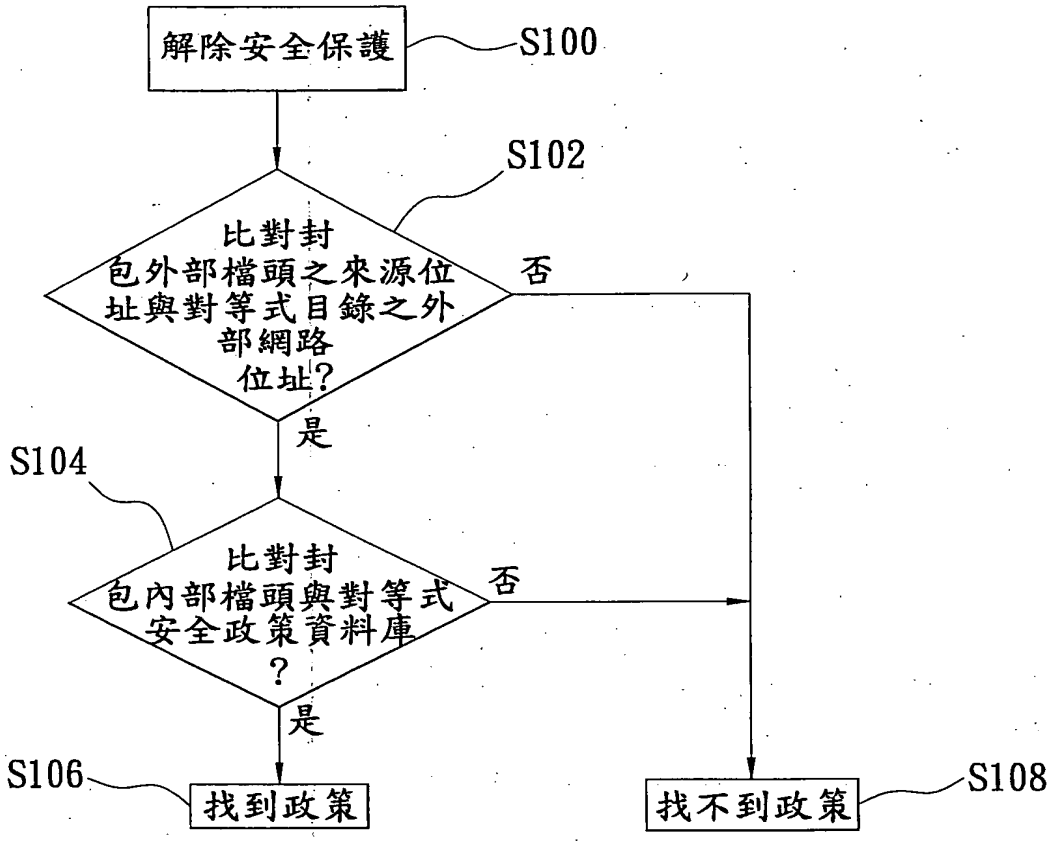
1 → SP1 → SP5

2 → SP2 → SP3 → SP4

0 → SP3

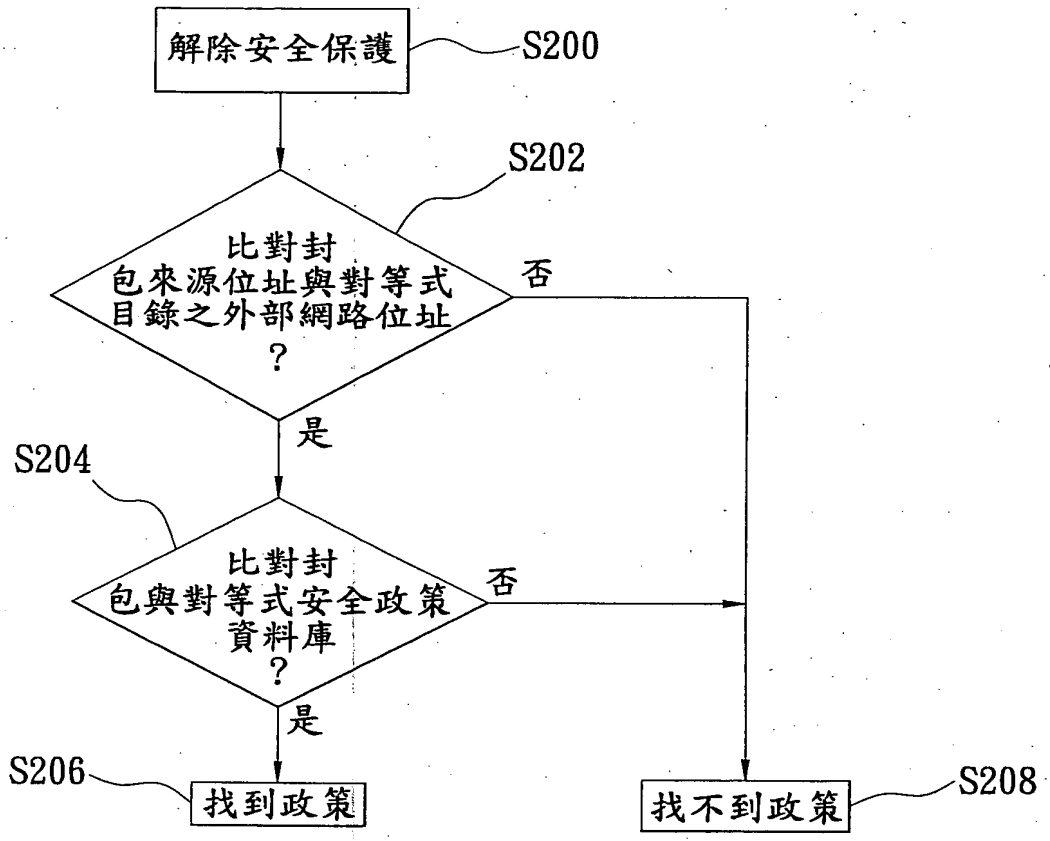
第八圖

圖式

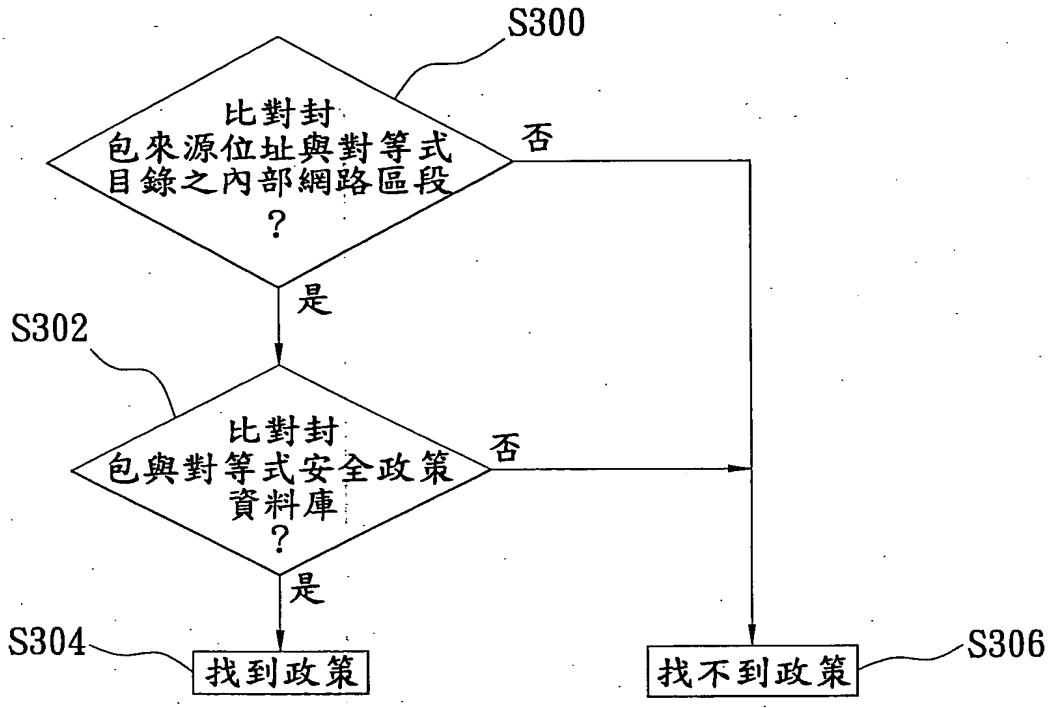

解除安全保護
S100
S102
比對封包外部檔頭之來源位址與對等式目錄之外部網路位址?
否
是
S104
比對封包內部檔頭與對等式安全政策資料庫?
否
是
S106
找到政策
找不到政策
S108

第九圖

圖式


解除安全保護
S200
S202
比對封包來源位址與對等式目錄之外部網路位址？
否
是
S204
比對封包與對等式安全政策資料庫？
否
是
S206
找到政策
找不到政策
S208

第十圖


S300
比對封包來源位址與對等式目錄之內部網路區段？
否
是
S302
比對封包與對等式安全政策資料庫？
否
是
S304
找到政策
找不到政策
S306

第十一圖